CONFIDENTIAL

ODP-81-1651
7 DEC 1981

MEMORANDUM FOR: Chief, [redacted] 25X1
25X1 [redacted]

VIA: Deputy Director for Administration

FROM: Bruce T. Johnson
Director of Data Processing

25X1 SUBJECT: Response to [redacted] Request for ADP Security Threat Assessment

25X1 REFERENCE: Memo from [redacted] dtd 17 November 1981

1. Attached is a draft reply to reference. It has been coordinated with the interested offices in the DDA; Data Processing, Logistics, and Security. We have not coordinated it with CI staff or any other component of the DDO.

2. If you have any questions, [redacted] 25X1
25X1 [redacted] is available to follow up on this reply.

[redacted] Bruce T. Johnson
25X1

Bruce T. Johnson

Attachment: a/s
cc: D/OL
D/OS
25X1 O/D/ODP [redacted] kf 07 December 1981

Distribution:
1 - Addressee w/att.
1 - DDA w/att.
1 - C/MS/P&PG w/att.
2 - O/D/ODP w/att.
2 - ODP Registry
1 - D/OL
1 - D/OS


CONFIDENTIAL
This Document becomes UNCLASSIFIED when separated from attachment.

Security Threat to ADP Systems During Acquisition

Reference: [redacted] 25X1
ADP Programmers - Possible Threat From Hostile Intelligence Service, dtd 17 Nov 81

We share your concerns, described in the reference, regarding the security of computer systems during acquisition. We regret that we are unable to provide quantitative estimates of the liklihood of the events you have described. It is our judgment, however, that both threats are real and must be defended against. [redacted] 25X1

Event (a) of your memorandum, describes the theft of hardware, software or documentation from a vendor's premises or while in transit. We presume here you are speaking of classified, and not commercially available unclassified ADP systems. We have in place an elaborate industrial security program to protect against the compromise of classified information, equipment or software from a contractor's facility. This program involves physical, technical, and personnel security initiatives. In addition, we have an industrial ADP security program to assure that information processing activities at a contractor's facility are protected from security compromise. [redacted] 25X1

We interpret event (b) of your memorandum to refer to the covert modification of nominally unclassified commercially available hardware or software. This would include, among other activities: modification to assist a covert penetration; modification to permit the covert capture of data for later removal; alteration of the emanations (TEMPEST) characteristics of the equipment; sabotage of the system (to cause random destruction of data, intermittent malfunction, etc.). The possibilities are only limited by the imagination of the adversary. Protection against this "Trojan Horse" attack is far more difficult because of the complexity of modern hardware and software and the uncontrolled nature of the commercial environment. Our approach to date involves dealing only with "trusted" vendors, using equipment in a secure environment with only security cleared personnel having access (including maintenance personnel), and enforcing rigorous TEMPEST standards. We recognize that these procedures may not be fully adequate and are continuously working to improve them. [redacted] 25X1

25X1

[redacted]

We do not consider the concerns you have raised academic. We know the Soviets have actively targeted the U.S. industrial community for covert activity. We further are aware that the Soviets continue to attempt to intercept transmissions between the U.S. Government and its contractors and vendors. To date, we are not aware of a Soviet success in the "Trojan Horse" scenario. Although they have, as you know, had success in the theft of classified information from nominally secure industrial
25X1 environments [redacted]

We are prepared to discuss these important matters further with your personnel at your convenience. Components of our Office of Security can provide information on industrial security policy and procedures. We are, of course, also prepared to discuss the general area of ADP security. With knowledge of the precise situation you are confronted with, we may be able to provide further assistance. [redacted] 25X1

We hope these comments have been helpful. We recognize that the area of ADP security is fraught with difficulties and administrative and technical challenges. We would appreciate any further thoughts you may have on these problems or our comments, or any additional experience you may have that you would like to
25X1 share with us. [redacted]